UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/646,716	08/25/2003	Thomas J. Kelly	08350.3304-01	9855

58982 7590 06/14/2007
CATERPILLAR/FINNEGAN, HENDERSON, L.L.P.
901 New York Avenue, NW
WASHINGTON, DC 20001-4413

EXAMINER	
HO, CHUONG T	
ART UNIT	PAPER NUMBER
2616	
MAIL DATE	DELIVERY MODE
06/14/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/646,716	**Applicant(s)** KELLY ET AL.	
	Examiner CHUONG T. HO	**Art Unit** 2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 September 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-46* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *04/ 2/04; 08/29/05*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This office action is in response to the Application SN 10/646,716 filed on 08/25/03. .Claim 1-46 are presented for examination.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 04/12/04; 08/29/05 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

3. The disclosure is objected to because of the following informalities: On the page 1, under section "Cross-Reference to Related Applications", the cited copending applications should be updated with current statuses such as U.S. Patent Application Serial No., the filing date, U.S. Patent No., and the issued date.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 45 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 45 appears to be a computer program claim which should constitute a computer instruction codes, however, the claim has method step being performed by a software code segment" interpreted as a software program. The claim taken as a whole appears to be a computer program being executed to software program. The claim taken as whole appears to be a computer program being executed which is non-statutory.

In the claim 45, “A computer-readable medium including instructions for performed a method in multi-protocol work machine environment, the method performed by a gateway and comprising” should be changed to - - A computer-readable medium encoded with computer program for performed in multi-protocol work machine environment, computer program executed by the computer and comprising - -;

5. Claim 46 appears to be a computer program claim which should constitute a computer instruction codes, however, the claim has method step being performed by a software code segment” interpreted as a software program. The claim taken as a whole appears to be a computer program being executed to software program. The claim taken as whole appears to be a computer program being executed which is non-statutory.

In the claim 46, “A computer-readable medium including instructions for performed a method in multi-protocol work machine environment, the method performed by a gateway and comprising” should be changed to - - A computer-readable medium encoded with computer program for performed in multi-protocol work machine environment, computer program executed by the computer and comprising - -;

Claim Rejections - 35 USC § 112

6. Claim 45 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 45 appears to be a computer program claim which

should constitute computer instruction codes, however, the claim has method steps being executed by an computer program segment interpreted as a software program. Therefore, it is not clear what is being claimed by the applicant is it the "a computer program " or a method system".

7. Claim 46 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 45 appears to be a computer program claim which should constitute computer instruction codes, however, the claim has method steps being executed by an computer program segment interpreted as a software program. Therefore, it is not clear what is being claimed by the applicant is it the "a computer program " or a method system".

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-2, 14-15, 33, 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meier (U.S.Patent No. 6,970,459 B1) in view of Selitrennikoff et al. (U.S.Patent No. 6,901,449 B1).

As to claim 1, Meier discloses a first module (figure 10, LNS) for sending a message, the first module (figure 1, LNS) coupled to first data link that uses a first protocol (L2TP, layer two tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

A second module (figure 10, MVTP client) for receiving the message over a second data link, the second data link using a second protocol (figure 10, MVTP, mobile VPN tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

A gateway (figure 10, VPN gateway) interconnecting the first and second data link and configured to:

Receive the message from the first data link in the first protocol (L2TP, layer two tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Determine whether the message is to be transmitted on the second data link based on an identifier included in the message (col. 12, lines 20-25, lines 31-36);

Encapsulate the message within a transmit unit consistent with the second protocol (col. 12, lines 31-36);

Transmit the encapsulated message to the second module (figure 10, MVTP client) over the second data link using the second protocol (figure 10, MVTP, mobile VPN tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Wherein the second module (figure 10, MVTP client) is configured to receive the encapsulated message from the second protocol transmission unit (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

However, Meier is silent to disclosing extract the message from second protocol transmission unit .

Selitrennikoff et al. discloses extract the message from second protocol transmission unit (figure 3, col. 4, lines 48-60, to extract the encapsulated data).

Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate extract the message from second protocol transmission unit taught by Selitrenikoff into the system of Meier. One would have been motivated to do so to facilitate transmission of information over an existing protocol without disrupting functionality associated therewith.

10. As to claim 14, Meier discloses a first on-board module (figure 10, LNS) for sending a message, the first on-board module (figure 1, LNS) coupled to first data link that uses a first protocol (L2TP, layer two tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

A second on-board module (figure 10, MVTP client) for receiving the message over a second data link, the second data link using a second protocol (figure 10, MVTP, mobile VPN tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

A gateway (figure 10, VPN gateway) interconnecting the first and second data link and configured to:

Receive the message from the first data link in the first protocol (L2TP, layer two tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Determine whether the message is to be transmitted on the second data link based on an identifier included in the message (col. 12, lines 20-25, lines 31-36);

Encapsulate the message within a transmit unit consistent with the second protocol (col. 12, lines 31-36);

Transmit the encapsulated message to the second module (figure 10, MVTP client) over the second data link using the second protocol (figure 10, MVTP, mobile VPN tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Wherein the second module (figure 10, MVTP client) is configured to receive the encapsulated message from the second protocol transmission unit (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

However, Meier is silent to disclosing extract the message from second protocol transmission unit .

Selitrennikoff et al. discloses extract the message from second protocol transmission unit (figure 3, col. 4, lines 48-60, to extract the encapsulated data). Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate extract the message from second protocol transmission unit taught by Selitrenikoff into the system of Meier. One would have been motivated to do so to facilitate transmission of information over an existing protocol without disrupting functionality associated therewith.

11. As to claim 33, Meier discloses output a message, by a source module (figure 10, LNS), on a first data link that uses a first protocol (L2TP, layer two tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

A gateway (figure 10, VPN gateway) interconnecting the first and second data link and configured to:

Receive, by the gateway, the message from the first data link in the first protocol (L2TP, layer two tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Determine whether the message is to be transmitted on the second data link based on an identifier included in the message (col. 12, lines 20-25, lines 31-36);

Encapsulate, by the gateway, the received message within a transmit unit consistent with the second protocol (col. 12, lines 31-36);

Output the encapsulated message on a second data link using the second protocol (figure 10, MVTP, mobile VPN tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Transmit the encapsulated message to the second module (figure 10, MVTP client) over the second data link using the second protocol (figure 10, MVTP, mobile VPN tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Wherein the second module (figure 10, MVTP client) is configured to receive the encapsulated message from the second protocol transmission unit (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

However, Meier is silent to disclosing extract the message from second protocol transmission unit .

Selitrennikoff et al. discloses extract the message from second protocol transmission unit (figure 3, col. 4, lines 48-60, to extract the encapsulated data). Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate extract the message from second protocol transmission unit taught by Selitrenikoff into the system of Meier. One would have been motivated to do so to facilitate transmission of information over an existing protocol without disrupting functionality associated therewith.

12. As to claim 34, As to claim 33, Meier discloses output a message, by a source module (figure 10, LNS), on a first data link that uses a first protocol (L2TP, layer two tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

A gateway (figure 10, VPN gateway) interconnecting the first and second data link and configured to:

Receive, by the gateway, the message from the first data link in the first protocol (L2TP, layer two tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Determine whether the message is to be transmitted on the second data link based on an identifier included in the message (col. 12, lines 20-25, lines 31-36);

Encapsulate, by the gateway, the received message within a transmit unit consistent with the second protocol (col. 12, lines 31-36);

Output the encapsulated message on a second data link using the second protocol (figure 10, MVTP, mobile VPN tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Transmit the encapsulated message to the second module (figure 10, MVTP client) over the second data link using the second protocol (figure 10, MVTP, mobile VPN tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Wherein the second module (figure 10, MVTP client) is configured to receive the encapsulated message from the second protocol transmission unit (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

However, Meier is silent to disclosing extract the message from second protocol transmission unit .

Selitrennikoff et al. discloses extract the message from second protocol transmission unit (figure 3, col. 4, lines 48-60, to extract the encapsulated data). Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate extract the message from second protocol transmission unit taught by Selitrenikoff into the system of Meier. One would have been motivated to do so to facilitate transmission of information over an existing protocol without disrupting functionality associated therewith.

13. As to claims 2, 15, Meier discloses the first data link is a proprietary data link (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36).

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. Claims 3-5, 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combined system (Meier – Selitrennikoff) in view of Akahane (7,054,319).

As to claims 3, 16, the combined system (Meier – Selitrennikoff) discloses the limitations of claim 1 above.

However, the combined system (Meier – Selitrennikoff) are silent to disclosing wherein the second data link is a non-proprietary data link including one of J1939, CAN, MODBUS, serial standard data link, and the Ethernet.

Akahane discloses wherein the second data link is a non-proprietary data link including one of J1939, CAN, MODBUS, serial standard data link, and the Ethernet. (col.2, lines 61-63, Ethernet).

Thus, one would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate wherein the second data link is a non-proprietary data link including one of J1939, CAN, MODBUS, serial standard data link, and the Ethernet taught by Akanhane into the combined system (Meier – Selitrennikoff). One would have been motivated to do so to enable VPN identification by using the identifiers of logical channels multiplexed and terminated to a physical interface.

16. As to claims 4, 17, Meier discloses wherein the gateway is further configured to discover, upon receiving the message from the first data link, that the first protocol is incompatible with the second protocol. (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36).

17. As to claims 5, 18, Meier discloses wherein the gateway is pre-configured to encapsulate messages received from the first data link within transmission units consistent with the second protocol (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Claim Rejections - 35 USC § 103

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

19. Claims 6-8, 9-13, 19-32, 39, 35, 36-38, 43, 44, 45, 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meier (U.S.Patent No. 6,970,459 B1) in view of Akahane et al. (U.S.Patent No. 7,054,319 B2).

As to claim 6, Meier discloses at least one destination module (figure 10, MVTP client) for receiving messages over a destination data link, the destination data link using a destination protocol (figure 10, MVTP, mobile VPN tunneling protocol) that is different from the source protocol (figure 10, L2TP, layer 2 tunneling protocol);

a gateway (figure 10, VPN gateway) interconnecting the source and destination data links and configured to: receiving message from the source data lines in the source protocol (L2TP, layer two tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Determine whether the message is to be transmitted on the second data link based on an identifier included in the message (col. 12, lines 20-25, lines 31-36);

Encapsulate the message within a transmit unit consistent with the second protocol (col. 12, lines 31-36);

Transmit the encapsulated message to the second module (figure 10, MVTP client) over the second data link using the second protocol (figure 10, MVTP, mobile VPN tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Wherein the second module (figure 10, MVTP client) is configured to receive the encapsulated message from the second protocol transmission unit (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Howerver, Meier is silent to disclosing a plurality of source data links, each using one of a plurality of source protocols.

Akanhane et al. discloses a plurality of source data links, each using one of a plurality of source protocols (figure 4, figure 12, col. 1, lines 35-40, lines 57-60, col. 2, lines 50-60).

Thus, one would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a plurality of source data links, each using one of a plurality of source protocols taught by Akanhane into the system of Meier. One would have been motivated to do so to enable VPN identification by using the identifiers of logical channels multiplexed and terminated to a physical interface.

20. As to claim 9, Meier discloses a source module (figure 10, LNS) for sending messages, the source module (figure 10, LNS) coupled to a source data link that uses a first protocol (L2TP; layer two tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

receiving messages over a destination data link, the destination data link using a destination protocol (figure 10, MVTP, mobile VPN tunneling protocol) that is different from the source protocol (figure 10, L2TP, layer 2 tunneling protocol);

a gateway (figure 10, VPN gateway) interconnecting the source and destination data links and configured to: receiving message from the source data lines in the source protocol (L2TP, layer two tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Determine whether the message is to be transmitted on the second data link based on an identifier included in the message (col. 12, lines 20-25, lines 31-36);

Encapsulate the message within a transmit unit consistent with the second protocol (col. 12, lines 31-36);

Transmit the encapsulated message to the second module (figure 10, MVTP client) over the second data link using the second protocol (figure 10, MVTP, mobile VPN tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Wherein the second module (figure 10, MVTP client) is configured to receive the encapsulated message from the second protocol transmission unit (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Howerver, Meier is silent to disclosing a plurality of destination data links, each destination data links using one of plurality of destination protocols, wherein the source and destination protocols are inconsistent.

Akanhane et al. discloses a plurality of destination data links, each destination data links using one of plurality of destination protocols, wherein the source and destination protocols are inconsistent (figure 4, figure 12, col. 1, lines 35-40, lines 57-60, col. 2, lines 50-60).

Thus, one would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a plurality of destination data links, each destination data links using one of plurality of destination protocols, wherein the source and destination protocols are inconsistent taught by Akanhane into the system of Meier. One would have been motivated to do so to enable VPN identification by using the identifiers of logical channels multiplexed and terminated to a physical interface.

21. As to claim 39, Meier discloses a translation table implemented in a memory device, the translation table including: at least one parameter identifier (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

A universal storage section for storing parameter data associated with the parameter identifier (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

A gateway (figure 10, VPN gateway) residing in a work machine configured to access the translation table (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36); wherein the gateway device: receiving a message, including a first parameter identifier and first parameter data, from the first data link used by the work machine, determined whether the first parameter matches the parameters in the translation table (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

When a match is found by the gateway, scaling the first parameter data using one of the plurality of scale factors that corresponds to a second data link protocol (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Outputting the scaled parameter data to a second data link using the second data link protocol (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36).

However, Meier is silent to disclosing a plurality of scale factors associated with the at least one parameters identifier, wherein each of the plurality of scale factors corresponds to a different data link protocol.

Akanhane et al. discloses a plurality of scale factors associated with the at least one parameters identifier, wherein each of the plurality of scale factors corresponds to a different data link protocol (figure 4, figure 12, col. 1, lines 35-40, lines 57-60, col. 2, lines 50-60).

Thus, one would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a plurality of scale factors associated with the at least one parameters identifier, wherein each of the plurality of scale factors corresponds to a different data link protocol taught by Akanhane into the system of Meier. One would have been motivated to do so to enable VPN identification by using the identifiers of logical channels multiplexed and terminated to a physical interface.

22. As to claim 35, claim 35 is rejected the same reasons of claim 39 above.

23. As to claim 36, claim 36 is rejected the same reasons of claim 39 above.

24. As to the claim 43, Meier discloses a source module (figure 10, LNS) for sending a source message coupled to a source data link that uses a first protocol (L2TP, layer two tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

A destination module (figure 10, MVTP Client) for receiving the source message, the source destination module (figure 10, MVTP Client) located at a distance from the source module (figure 10, LNS) that exceeds a transmission range of the first protocol (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

A first gateway coupled to the source data link and an intermediate data link, the intermediate data link using a second protocol (MVTP), the first gateway configured to: receive the message from the source data link in the first protocol (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Encapsulate the message within a transmission unit consistent with the second protocol (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

However, Meier is silent to disclosing a second gateway coupled to the intermediate data link and the destination module, the second gateway configured to: receiving the encapsulated message from the intermediate data link; extract the source message from the second protocol transmission unit; and route the source message to the destination module.

Akahane et al. discloses a first gateway (figure 1, 9) a second gateway (figure 1, 10) coupled to the intermediate data link and the destination module, the second gateway configured to: receiving the encapsulated message from the intermediate data link; extract the source message from the second protocol transmission unit; and route the source message to the destination module (An ISP network (5) has edge routers (9 and 10) positioned at the boundaries of the network and a core router (17) positioned in the core of the network. Although a single core router (17) is shown in FIG. 1, the number of core routers is not limited to one. Datagrams are assumed to be encapsulated by MPLS (for ATM) to pass across the ISP network (5), thus implementing reliable data transmission across VPNs. Not only this encapsulation protocol but also other encapsulation protocols mentioned above may be used. The ISP network (5) interconnects LAN1 (1) and LAN2 (2) via the edge router (9) and LAN3 (3) and LAN4 (4) via the edge router (10). The LAN1 (1) and the LAN3 (3) are assumed to be possessed by corporation A and one VPN is formed to cover these LANs. The LAN2 (2) and the LAN4 (4) are assumed to be possessed by corporation B and another VPN is formed to cover these LANs. The corporation A's VPN is to be called VPNA (7) and the corporation B's VPN is VPNB (8).) (When the lower layer processor (53) receives a packet from a LAN, it terminates the lower layer protocol below IP for the packet. To a packet forwarding processor (101), the lower layer processor (53) transfers the IP packet and the information relevant to the packet including the physical interface number at which the packet was received (hereinafter referred to as a receiving physical interface number), the lower layer protocol type, and the capsule header information for the lower layer to be used as the VPN identifier. The packet forwarding processor (101) extracts the IP header information from the IP packet it received and transfers the IP header information, the receiving physical interface number, the lower layer protocol type, and the capsule header information for the lower layer to be used as the VPN identifier to a VPN identification table/routing table look-up processor (102). The IP packet itself is temporally accumulated in the packet forwarding processor (101)).

Thus, one would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a second gateway coupled to the intermediate data link and the destination module, the second gateway configured to: receiving the encapsulated message from the intermediate data link; extract the source message from the second protocol transmission unit; and route the source message to the destination module taught by Akanhane into the system of Meier. One would have been motivated to do so to enable VPN identification by using the identifiers of logical channels multiplexed and terminated to a physical interface.

25. As to claim 44, Meier discloses a source module (figure 10, LNS) for sending a source message coupled to a source data link that uses a first protocol (L2TP, layer two tunneling protocol) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

A destination module (figure 10, MVTP Client) for receiving the source message, the source destination module (figure 10, MVTP Client) located at a distance from the source module (figure 10, LNS) that exceeds a transmission range of the first protocol (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

A first gateway coupled to the source data link and an intermediate data link, the intermediate data link using a second protocol (MVTP), the first gateway configured to: receive the message from the source data link in the first protocol (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

Encapsulate the message within a transmission unit consistent with the second protocol (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36);

However, Meier is silent to disclosing a second gateway coupled to the intermediate data link and the destination module, the second gateway configured to: receiving the encapsulated message from the intermediate data link; extract the source message from the second protocol transmission unit; and route the source message to the destination module.

Akahane et al. discloses a first gateway (figure 1, 9) a second gateway (figure 1, 10) coupled to the intermediate data link and the destination module, the second gateway configured to: receiving the encapsulated message from the intermediate data link; extract the source message from the second protocol transmission unit; translate the extracted message into a comparable message of a destination protocol by a destination data link coupled to the destination module; and and route the translated message to the destination module over the destination data link (An ISP network (5) has edge routers (9 and 10) positioned at the boundaries of the network and a core router (17) positioned in the core of the network. Although a single core router (17) is shown in FIG. 1, the number of core routers is not limited to one. Datagrams are assumed to be encapsulated by MPLS (for ATM) to pass across the ISP network (5), thus implementing reliable data transmission across VPNs. Not only this encapsulation protocol but also other encapsulation protocols mentioned above may be used. The ISP network (5) interconnects LAN1 (1) and LAN2 (2) via the edge router (9) and LAN3 (3) and LAN4 (4) via the edge router (10). The LAN1 (1) and the LAN3 (3) are assumed to be possessed by corporation A and one VPN is formed to cover these LANs. The LAN2 (2) and the LAN4 (4) are assumed to be possessed by corporation B and another VPN is formed to cover these LANs. The corporation A's VPN is to be called VPNA (7) and the corporation B's VPN is VPNB (8).) (When the lower layer processor (53) receives a packet from a LAN, it terminates the lower layer protocol below IP for the packet. To a packet forwarding processor (101), the lower layer processor (53) transfers the IP packet and the information relevant to the packet including the physical interface number at which the packet was received (hereinafter referred to as a receiving physical interface number), the lower layer protocol type, and the capsule header information for the lower layer to be used as the VPN identifier. The packet forwarding processor (101) extracts the IP header information from the IP packet it received and transfers the IP header information, the receiving physical interface number, the lower layer protocol type, and the capsule header information for the lower layer to be used as the VPN identifier to a VPN identification table/routing table look-up processor (102). The IP packet itself is temporally accumulated in the packet forwarding processor (101)).

Thus, one would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a second gateway coupled to the intermediate data link and the destination module, the second gateway configured to: receiving the encapsulated message from the intermediate data link; extract the source message from the second protocol transmission unit; and route the source message to the destination module taught by Akanhane into the system of Meier. One would have been motivated to do so to enable VPN identification by using the identifiers of logical channels multiplexed and terminated to a physical interface.

26. As to claim 9, claim 9 is rejected the same reasons of claim 43 above.

27. As to claim 7, Akahane discloses wherein the destination module is configured to receive the encapsulated messages and extract the message from destination protocol transmission unit (FIG. 1 is a schematic diagram for explaining a preferred embodiment

of forming VPNs interconnected by VPN edge routers according to the present invention. Hereinafter, a lower layer will mean a protocol for encapsulating datagrams in IP packets. Even if an IP header is used to encapsulate datagrams of IP packets, this capsule header will be represented as a lower layer header for convenience.) (The packet forwarding processor (101) extracts the IP header information from the IP packet it received and transfers the IP header information, the receiving physical interface number, the lower layer protocol type, and the capsule header information for the lower layer to be used as the VPN identifier to a VPN identification table/routing table look-up processor (102). The IP packet itself is temporally accumulated in the packet forwarding processor (101)).

28. As to claim 8, Meier discloses wherein the gateway receives and encapsulates the messages simultaneously (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36).

29. As to claim 10, claim 10 is rejected the same reasons of claim 7 above.

30. As to claim 11, claim 11 is rejected the same reasons of claim 8 above.

31. As to claim 12, Meier disclose where the source data link is a proprietary data link (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36).

32. As to claim 13, Akahane discloses wherein the destination data links are non-proprietary standard data links (col. 2, lines 61-63, Ethernet).

33. As to claim 20, Akahane discloses a destination data link coupled to the second gateway and the destination module for transporting messages from the second gateway (figure 1, 10) to the destination module (figure 1, enterprise A, enterprise B) (col. 2, lines 50-60).

34. As to claim 21, Akahane discloses wherein the destination data link uses the source protocol (col. 2, lines 50-60).

35. As to claim 22, Akahane discloses wherein the first gateway (figure 1, 9) is configured to encapsulate, upon receiving the source message, that the source message is to be encapsulated within the second protocol transmission unit (col. 2, lines 50-60).

36. As to claim 23, Akahane discloses the first gateway (figure 1, 9) determines to encapsulate the source message by way of examining a destination identifier included in the source message (col. 2, lines 50-60).

37. As to claims 24, 37, 40, Meier discloses the source data link is a proprietary data link (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36).

38. As to claims 25, 38, 41, 42, Akahane discloses wherein the intermediate data link is a non-proprietary standard data link including one of a J1939, CAN, MODBUS, serial standard data link, and the Ethernet (col.2, lines 61-63, Ethernet).

39. As to claim 26, Meier discloses wherein the source module is an on-board module located within a first work machine (figure 10) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36).

40. As to claim 27, Meier discloses wherein the destination module is an on-board located within the first work machine (figure 10) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36).

41. As to claim 28, Meier discloses wherein the destination module is an off-board module located external to the first work machine (figure 10) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36).

42. As to claim 29, Akahane discloses wherein the second gateway (figure 1, 10) is located external to the first work machine (col. 2, lines 50-60).

43. As to claim 30, Meier discloses wherein the source module is an off-board module (figure 10) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36).

44. As to claim 31, Meier discloses wherein the destination module is an off-board module (figure 10) (col. 11, lines 65-67, col. 12, lines 20-25, lines 31-36).

45. As to claim 32, Akahane discloses wherein the second gateway (figure 1, 10) is located within the first work machine (col. 2, lines 50-60).

46. As to claim 45, claim 45 is rejected the same reasons of claim 35 above.

47. As to claim 46, claim 46 is rejected the same reasons of claim 36 above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHUONG T. HO whose telephone number is (571) 272-3133. The examiner can normally be reached on 8:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Huy Vu can be reached on (571) 272-3155. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

06/12/07

HUY D. VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600